

09/913213

REF: 8/10/01 290.796USN

EXPRESS MAIL LABEL NO. EL675381865US

Date of Mailing: 10 August 2001

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE
(DO/EO/US) CONCERNING FILING UNDER 35 U.S.C. 371

Attorney Docket No.: 290.796USN

Int'l. Application No.: PCT/FI00/00075
 Int'l. Filing Date: 2 FEB 2000
 Priority Date Claimed: 10 FEB 1999
 Title of Invention: DATA COMMUNICATION METHOD FOR
 SENDING A MESSAGE THROUGH A
 FIREWALL
 Applicant(s) for DO/ES/US: Panu Pietikainen

Applicant herewith submits to the United States
 Designated/Elected/Office (DO/EO/US) the following items and
 other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 37 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) (unsigned).
11. ☐ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.
12. ☐ An assignment document for recording. A cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.

00913213.0129002

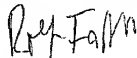
Date of Mailing: 10 August 2001

13. [X] A FIRST preliminary amendment.
14. [X] Applicant qualifies for Small Entity Status (37 C.F.R. 1.9(E) and 1.27(b)).
16. [] Other items or information: (if any)
17. [X] Basic National Filing Fee of \$1000.00 is submitted (Neither international preliminary examination fee (37 C.F.R. 1.462) nor international search fee 37 C.F.R. 1.44.5(a)(2) paid to U.S.P.T.O.).

CLAIMS AS FILED			
For	Number Filed	Number Extra	Basic Fee \$1000.00 Rate
Total Claims	10 - 20	= 0	x \$18.00 = \$0.00
Ind. Claims	1 - 3	= 0	x \$80.00 = \$0.00

19. [X] Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity.
TOTAL FILING FEE: \$500.00.
20. [] Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property.
21. [X] A check in the amount of \$500.00 to cover the above fees is enclosed.
23. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 05-0243.

Respectfully submitted,



Rolf Fasth
Registration Number 36,999

Send all correspondence to:

Rolf Fasth, Esq.
FASTH LAW OFFICES
5255 Camelot Forest Drive
Jacksonville, FL 32258-2516

Telephone: (904) 288-0262
Facsimile: (904) 288-0263

cc: Paivi Söderman
(Your Ref. S0010US)

09/913213

JCO5 Rec'd PCT/PTO 10 AUG 2001

EXPRESS MAIL LABEL NO. EL675381865US
Date of Mailing: 10 August 2001

#4/a

EP:83 8/10/01 296.796US\$

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit

Panu PIETIKAINEN

Serial No.

Filed: Herewith

For: DATA COMMUNICATION
METHOD FOR SENDING A
MESSAGE THROUGH A
FIREWALL

Examiner:

Date: 10 August 2001

PRELIMINARY AMENDMENTAssistant Commissioner for Patents
Washington, DC 20231Preliminary to examination, please amend the above-
identified patent application as follows:In the claims:

1. A method for sending a message from a first computer system C1 that belongs to an internal network, which is protected by a firewall to at least one other computer system C2 through the firewall comprising:
 - a) sending from the first computer system to the firewall, a request with data for a new connection to be opened between the first computer system C1

09/913213.012902

- and at least one other computer system C2 for a message to be sent between said computer systems C1, C2,
- b) the firewall controls the data for the new connection via which the message is intended to be sent and, up on approval of the connection by the firewall, sending from the firewall to the first computer system C1, information about the necessary modifications to be made in a message that is sent via the requested connection through the firewall, so that the message can pass through, the necessary modifications including IP, protocol, TCP and/or port data,
- c) modifying, by the first computer system C1, the message to be sent in accordance with the information sent from the firewall,
- d) optionally, and before or after step c), sending from the first computer system C1 to the firewall identification data of the connection for the message to be sent between said computer systems C1, C2 so that the connection for the message can be identified by the firewall and the message can pass the firewall,

09913213-0129002

RF:ej 8/10/01 290.196DSN

PATENT

- e) sending the message from the first computer system C1 to the at least one other computer system C2 through the firewall.

2. The method according to claim 1 wherein the message to be sent between said computer systems C1, C2 is protected in step c) after it has been modified, whereby step d) is necessary and the data to be sent from the first computer system C1 to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

3. The method according to claim 2 wherein the protection is made using the IP Sec system.

4. The method according to claim 2 wherein the message to be sent is authenticated.

5. The method according to claim 2 wherein the message to be sent is encrypted in step c).

6. The method according to claim 1 wherein the information message in point a) contains data of the new connection to be opened between the first computer system C1 and at least one other computer system C2 in form of address identification data and possible other parameters.

000133213 012900

EP:8] 8/10/01 299.796USN

PATENT

7. The method according to claim 6 wherein the possible other parameters are data about the port and the protocol used for sending.

8. The method according to claim 1 wherein in step b) the modifications include address identification data and/or the port and or the protocol used for sending.

9. The method according to claim 1 wherein the message is using the TCP/IP protocol.

10. The method according to claim 1 wherein the message is sent via internet.

REMARKS

Reconsideration of the application is respectfully requested. The claims have been amended so that the application better conforms to U.S. Patent Practice. A copy of the marked-up amended claims is attached as Appendix A.

An abstract on a separate page has been added as Appendix B.

00013213.012902

EXPRESS MAIL LABEL NO. EL675381865US
Date of Mailing: 10 August 2001

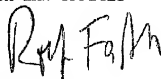
RF:sj 8/10/01 290.796US\$

PATENT

The application is submitted to be in condition for
allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES



Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
5255 Camelot Forest Drive
Jacksonville, FL 32258-2516

Telephone: (904) 288-0262
Facsimile: (904) 288-0263

cc: Paivi Söderman
(Your Ref. S0010US)

09913613 012902

09/913213

09 AUG 2001

EXPRESS MAIL LABEL NO. EL675381865US
Date of Mailing: 10 August 2001

RF:BJ 8/10/01 290.736USR

PATENT

APPENDIX A
Marked-Up Claims

1. [Method] A method for sending a message from a first computer system C1 that belongs to an internal network, which is protected by a firewall to at least one other computer system C2 through the firewall [characterized in the following steps] comprising:

- a) sending from the first computer system to the firewall, a request with data for a new connection to be opened between the first computer system C1 and at least one other computer system C2 for a message to be sent between said computer systems C1, C2,
- b) the firewall controls the data for the new connection via which the message is intended to be sent and, up on approval of the connection by the firewall, sending from the firewall to the first computer system C1, information about the necessary modifications to be made in a message that is sent via the requested connection through the firewall, so that the message can pass through, the necessary modifications including IP, protocol, TCP and/or port data,

09/913213.012902

RP:SJ 8/10/01 230.796DSN

PATENT

- c) modifying, by the first computer system C1, the message to be sent in accordance with the information sent from the firewall,
- d) optionally, and before or after step c), sending from the first computer system C1 to the firewall identification data of the connection for the message to be sent between said computer systems C1, C2 so that the connection for the message can be identified by the firewall and the message can pass the firewall,
- e) sending the message from the first computer system C1 to the at least one other computer system C2 through the firewall.

2. [Method of claim 1, characterized in that,] The method according to claim 1 wherein the message to be sent between said computer systems C1, C2 is protected in step c) after it has been modified, whereby step d) is necessary and the data to be sent from the first computer system C1 to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

3. [Method of claim 2, characterized in that] The method according to claim 2 wherein the protection is made using the IP Sec system.

00013213-012000

RF:aj 8/10/01 290.798USN

PATENT

4. [Method of claim 2 or 3, characterized in that]

The method according to claim 2 wherein the message to be sent is authenticated.

5. [Method of any of claims 2 - 4, characterized in

that] The method according to claim 2 wherein the message to be sent is encrypted in step c).

6. [Method of any of claims 1 - 5, characterized in

that] The method according to claim 1 wherein the information message in point a) contains data of the new connection to be opened between the first computer system C1 and at least one other computer system C2 in form of address identification data and possible other parameters.

7. [Method of claim 6, characterized in that] The

method according to claim 6 wherein the possible other parameters are data about the port and the protocol used for sending.

8. [Method of any claims 1 - 7, characterized in

that] The method according to claim 1 wherein in step b) the modifications include address identification data and/or the port and or the protocol used for sending.

9. [Method of any claim 1 - 7, characterized in

that,] The method according to claim 1 wherein the message is using the TCP/IP protocol.

00013213 012002

EXPRESS MAIL LABEL NO. EL675381865US
Date of Mailing: 10 August 2001

RF:Sj 8/10/01 290.796USN

PATENT

10. [Method of any claim 1 - 8, characterized in
that,] The method according to claim 1 wherein the message is
sent via internet.

09913213.012902
200210.0722160

APPENDIX B

ABSTRACT

The invention is concerned with a method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall. The method comprises the following steps: a request with data for a new connection between the first computer system and at least one other computer system is sent from the first computer system to the firewall for a message to be sent between said computer systems. Upon approval of the connection by the firewall, information about necessary modifications to be made in a message that is sent via the requested connection through the firewall is sent from the firewall to the first computer system. The message to be sent is modified in the first computer system in accordance with the information sent from the firewall.

20020810 012200

DATA COMMUNICATION METHOD FOR SENDING A MESSAGE THROUGH A FIREWALL

5 TECHNICAL FIELD

The invention is concerned with a data communication method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall. The method can be used for sending protected
10 messages with various kinds of protection methods, computer networks and network protocols and is expected to be very useful for instance for sending secret messages.

15 DESCRIPTION OF RELATED ART

A computer network is formed when two or more computers are connected to each other. Local area networks (or internal networks) may be formed of the computers within a company, while wide area networks may be extended over bigger areas,
20 such as many towns and even countries. The networks may be connected via cables, fibers and/or radio links.

An example of a global network is the Internet. This worldwide network can be used for communication, delivering and searching for information.

25 If an internal system for electronic post is installed, everyone connected to the local network can send messages to each other. The local network can be connected to another network, which can be an external network, such as Internet, and so electronic mail can be sent to the whole world to everyone connected to the external network. Internet is the most common network for data communication, by
30 for example E-mail.

New description
New claims

AMENDED SHEET. ENCLOSURE I

The fact that several local networks can be connected to other networks, Internet in particular, sets up requirements for the security and the equipment therefor.

There are different systems for the improving of the security. It is important that data within an internal network is protected so that only right users can change and read it. The users usually identify themselves with a user name and a password. Also other security details exist. Other security problems are network errors and work stops. With increasing complexity, advanced security systems become important.

The popularity of Internet can be seen on the fact that new network products and services are developed all the time. These products are developed in accordance with new Internet standards and are applied to the protocols used in transfers on Internet.

A firewall is a security system to protect a network against infringement from unauthorized users in other networks, such as Internet. A firewall can hinder computers from communicating directly with other networks, such as external networks, and vice versa. Instead, all communication is sent through the firewall placed outside the internal network. The firewall decides if it is safe to let messages and files pass between the external and the internal network on the basis of the addresses of the message, that can be in form of data packets, and different parameters. The firewall thus controls the communication between the internal and external network and modifies the data packets of for example TCP/IP based Internet (with respect to the TCP/IP protocol, see the next page). Usually, a firewall translates network addresses and other data defining the communication so that the internal address and the internal parameters are changed to an external address and external parameters. This means that for instance IP addresses used in an internal or local network are hidden from outside users. A packet coming from an external network to an internal network is modified back by the firewall.

The firewall can be formed in many different ways and is usually designed individually from case to case in accordance with the actual needs of the network. If the amount of traffic through the firewall is very high, quite extensive hardware for the firewall computer is needed.

Another method of increasing the security is by means of protection of the messages to be sent by for instance tunneling in virtual networks. In virtual networks several local and global networks use Internet to be connected to each other. By tunneling, data is transferred between two networks via a third network, such as Internet. In this technique, a given kind of data packets of a given protocol is encapsulated in packets of another protocol. Packet mode is a transfer method that can be used in virtual connections. In this technique data is sent in small "packets" with an address and a sender, so that several persons can use the connection simultaneously. The other protocol is usually TCP/IP, when the transfers go through Internet. The own protocols are packed in the TCP/IP packages that are sent via Internet.

The data communication between computers is carried out according to given rules which are called protocols TCP/IP is one such protocol and is an abbreviation for Transmission Control Protocol/Internet Protocol. Standards for TCP/IP are well documented in so called RFC (Request for comments) documents. The IP protocol takes care of the data packets and is responsible for that the packets find right addresses. The data packets are addressed by means of internet addresses and go from computer to computer until the right destination is reached. Communication with IP is connectionless as no fixed connection exist between communicating computers. The message is going forward step by step. The TCP protocol takes care of the transferring of messages between two computers by making a virtual connection between them without any physical connection. The TCP is the transport protocol that is responsible for the connection itself between sender and receiver. Also other standards than TCP/IP can be used in Internet.

The packets go through the "tunnel" maintained by Internet to the receiver, where the packets of different protocols are separated from each other and return to the original form. The authorization of the receiver can be controlled in different ways. The authorization control can be carried out in two steps: authentication and
5 authorization. Authentication is carried out to control the identity of the user, while the authorization defines what the user is authorized to do.

The virtual networks give a high security. The secret information has an own channel on Internet as a result of different methods of authentication, encryption
10 and/or encapsulation.

The security of Internet is not sufficient for all types of transfers. There are however ways to protect e-mail and other messages sent through internet from others. Especially high security can be achieved by encryption.
15

Encryption means that messages are changed before sending so that they cannot be read before decryption with a special key and usually also by confirming that the right person sent the message (authentication). There are a big variety of encryption methods of the above kind.
20

In many protection methods all connections have different parameters. The function wherein the real protection is made is called transformation. In the transformation function the packet is changed in accordance with given parameters depending on the actual protection used.
25

One problem with firewalls is the need of extensive equipment for the firewall computer if the traffic amount of traffic through the firewall is high.

Another problem with firewalls is that if protection methods are used and the
30 network is protected with a firewall, the firewall cannot identify the messages to be sent and will therefore not let them pass.

In existing methods, the protection function or the parameters for the protection are given to the firewall so that the firewall can identify or protect the message and the message can then be sent through the firewall. The drawback with such methods is decreased security for the local network as secret information is delivered outside the local network.

US patent 0715668 is mentioned as such prior art. The patent is about secure transfer of information between firewalls over an unprotected network. Internet protocol security and IPSec messages are handled in the firewall without assuming that encrypted messages has access to all services by decrypting the message and controlling the access. Another such method is described in US patent 0586231, wherein a firewall computer is allowed to provide virtual tunnel records and secret keys. Further examples of documents, wherein the firewall has encryption functions are UK Patent Application GB 2 317 792 and WO publication 97 00 471.

In the European patent application EP 0 858 201 an electronic data transfer system transmits a message between the first computer system, arranged within a firewall, and a second computer system. Messages that are not suitable for transmission through a firewall are translated in a format that is appropriate for transmission across the firewall.

THE OBJECT OF THE INVENTION

An object of the invention is a method of sending messages that decreases the work to be done by the firewall computer compared with previously known methods.

The second object of the invention is a safer method of sending protected messages through a firewall.

More in detail, the second object of the invention is a method wherein protected messages can be sent through a firewall without delivering information about the parameters of the protection outside the local network to the firewall.

5

DESCRIPTION OF THE INVENTION

In the method of the invention a message is sent from a first computer system that belongs to an internal network, which is protected by a firewall to at least one other
10 computer system through the firewall. In step a), a request with data for a new connection to be opened between the first computer system and at least one other computer system is sent from the first computer system to the firewall. In step b), the firewall controls the data for the new connection via which the message is intended to be sent and, up on approval of the message by the firewall, information
15 about the necessary modifications to be made in a message that is sent via the requested connection through the firewall is sent from the firewall to the first computer system so that the message can pass through. The necessary modifications include IP, protocol, TCP and/or port data. In step c), the protected message to be sent is modified in the first computer system in accordance with the information sent from the firewall. In step d), which is optional and can be carried
20 out before step c) or after step c), identification data of the connection for the message to be sent between said computer systems is sent to the firewall so that the message can be identified by the firewall to be able to pass the same. In step e), the protected message is then sent from the first computer system to the at least
25 one other computer system through the firewall.

In an application of the method, the message to be sent is protected as the method is very suitable for sending protected messages. The message to be sent between said computer systems is in that case protected in step c) after it has been
30 modified, whereby step d) is necessary and the data to be sent from the first

computer system to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

The protection method can be some method known in the art. One suitable way to protect the message is to use methods defined in the standard RFC 1825 for TCP/IP. This standard includes sub standards for for instance authentication methods and encryption methods, which can be used separately or simultaneously in a message sent with the method of the invention. RFC 1825 is a standard defining the IPSec security system standard, which consists of technology principles for the method used. IPSec, in turn, has sub standards for encryption, such as ESP, which is an abbreviation for encapsulated security protocol and AH, which is an abbreviation for a standard in IP for authentication. The authentication method might be MD5, SHA or other method known in the art. The encryption method might be some known method such as DES, Blowfish or the like.

In step a), the request for a new communication sent from the first computer system to the firewall contains for instance data of the new connection to be opened between the first computer system and at least one other computer system in for example in form of address identification data and such other parameters. Typical other parameters are for instance IP Data (the sender address, the receiver address), the type of protocol and TCP data: the sender port and the receiver port. The port defines the application for sending the data with e.g. TCP/IP, such as the program used, the web browser etc.

In step b), typical parameters that the firewall modifies so that the messages can pass through are the above data, for instance IP Data (the sender address, the receiver address), the type of protocol and TCP data: the sender port and the receiver port. The modifications might comprise all data of step a) or a part of them. All of the data to be modified might be known by the firewall even if not exactly included in step a).

Messages can only go through a firewall if the firewall can identify them to be allowable messages. In step d), identification data for the protection used to protect the message to be sent between said computer systems is sent to the firewall so that the protected message can be identified by the firewall. The identification data is in such a form that the firewall can identify the actual connection but not the actual parameters that have been used to protect the message. There exist many allowed connections with the same IP address but different other parameters. The actual protected message is sent in accordance with the parameters of one of the allowed connections and shall be identified by the firewall as being allowed and safe to deliver. If the message is not protected, step d) might be unnecessary in some embodiments, but is still advantageous to carry out in other embodiments, for instance if much traffic is going through the firewall, step d) might speed up the sending.

In the invention, the inventive idea is that a part of the firewall functionality has been given to another computer function and is carried out in the first computer system. If the message is protected, the firewall and the first computer system transfers necessary information so that the firewall would be able to pass the protected messages without having knowledge about the actual parameters used to protect the message to be sent.

In the following, the invention is described by means of some preferred embodiments of the invention. The details of the embodiments can vary within the scope of the claims.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a flow sheet over the different steps of the method of invention

Figure 2 is a schematic view of the computer network within which the data communication of the invention is carried out

5 DETAILED DESCRIPTION OF THE INVENTION

Figure 2 is a schematic view of a computer network within which the data communication of the invention can be carried out. A message shall be sent from a first computer system C1 to a second computer system C2.

10 In figure 2, the first computer system belongs to an internal network. The internal network is protected by a firewall, so that all messages to be sent and received through the firewall has to be identified and accepted by the firewall.

The firewall controls data of the connection via which the messages are sent and if the connection is accepted by the firewall, the messages can pass the firewall.

15 Before the messages can pass the firewall, they are modified in the firewall in accordance with given parameters, such as address changes and protocol changes. The computer system C1 has a virtual connection to computer system C2, which means that messages to be sent from the first computer system C1 to the second computer system C2 are sent via one or more other networks, such as
20 external networks, for instance Internet, after having passed the firewall before ending up at and received by the second computer system C2.

Figure 1 is a flow sheet over the different steps of an embodiment of the method of the invention. A message shall be sent on a computer network from the first
25 computer system C1 to a second computer system C2 through a firewall, which is placed outside the internal or local network to which the first computer system C1 belongs. The method of the invention can be used both for the purpose to decrease the work to be carried out by the firewall and/or for sending protected messages. If the message to be sent shall be protected before sending in accordance with the
30 second embodiment of the invention, it can not be sent through the firewall in the normal way, because the firewall is not able to control address identification data of

protected messages or forward encrypted messages. Therefor, in accordance with step a) of the invention, an information message is sent from the first computer system C1 to the firewall containing data about a new connection between the first computer system C1 and a second computer system C2 system in form of for instance address identification data, and possible other parameters for the message to be sent between said computer systems. If the firewall accepts this connection, the sending proceeds so that according to step b), information about necessary changes to be made in the message is sent from the firewall to the first computer system C1 so that the message can be sent through the firewall. The message that is intended to be protected with some protection method, that can be an authentication method and/or encryption method and shall be sent is according to step c) first modified by the first computer system C1 in accordance with the information sent from the firewall before protection. Before the protected message is sent, identification data of the protection method that have been used for protection of the message is according to point d) sent from the first computer system C1 to the firewall F so that the protected message can be identified but not read by the firewall to be able to be passed by the same. If the message is not protected, step d) is optional if the firewall used is able to identify the message. Step d) can also be carried out before step c). The protected message is then according to step e) sent from the first computer system C1 to the other computer system C2 through the firewall.

CLAIMS

1. Method for sending a message from a first computer system C1 that belongs to an internal network, which is protected by a firewall to at least one other computer system C2 through the firewall, characterized in the following steps:

- a) sending from the first computer system to the firewall, a request with data for a new connection to be opened between the first computer system C1 and at least one other computer system C2 for a message to be sent between said computer systems C1, C2,
- b) the firewall controls the data for the new connection via which the message is intended to be sent and, up on approval of the connection by the firewall, sending from the firewall to the first computer system C1, information about the necessary modifications to be made in a message that is sent via the requested connection through the firewall, so that the message can pass through, the necessary modifications including IP, protocol, TCP and/or port data,
- c) modifying, by the first computer system C1, the message to be sent in accordance with the information sent from the firewall,
- d) optionally, and before or after step c), sending from the first computer system C1 to the firewall identification data of the connection for the message to be sent between said computer systems C1, C2 so that the connection for the message can be identified by the firewall and the message can pass the firewall,
- e) sending the message from the first computer system C1 to the at least one other computer system C2 through the firewall.

2. Method of claim 1, characterized in that, the message to be sent between said computer systems C1, C2 is protected in step c) after it has been modified, whereby step d) is necessary and the data to be sent from the first computer system C1 to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

3. Method of claim 2, characterized in that the protection is made using the IP Sec system.

4. Method of claim 2 or 3, characterized in that the message to be sent is authenticated.

5. Method of any of claims 2 – 4, characterized in that the message to be sent is encrypted in step c).

6. Method of any of claims 1 – 5, characterized in that the information message in point a) contains data of the new connection to be opened between the first computer system C1 and at least one other computer system C2 in form of address identification data and possible other parameters.

7. Method of claim 6, characterized in that the possible other parameters are data about the port and the protocol used for sending.

8. Method of any of claims 1 - 7, characterized in that in step b) the modifications include address identification data and/or the port and or the protocol used for sending.

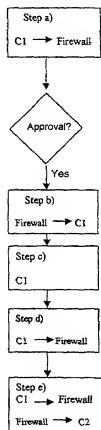
9. Method of any of claim 1 – 7, characterized in that, the message is using the TCP/IP protocol.

10. Method of any of claim 1 – 8, characterized in that, the message is sent via internet.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 29/06, G06F 17/60	A1	(11) International Publication Number: WO 00/48372 (43) International Publication Date: 17 August 2000 (17.08.00)
(21) International Application Number: PCT/FI00/00075 (22) International Filing Date: 3 February 2000 (03.02.00) (30) Priority Data: 990265 10 February 1999 (10.02.99) FI (71) Applicant (for all designated States except US): INTRASE- CURE NETWORKS OY [FI/FI]; P.O. Box 18, FIN-02151 Espoo (FI). (72) Inventor; and (73) Inventor/Applicant (for US only): PIETIKÄINEN, Panu [FI/FI]; Täysikuu 10 C 103, FIN-02210 Espoo (FI). (74) Agent: INNOPAT LTD; P.O. Box 556, FIN-02151 Espoo (FI).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i>
(54) Title: DATA COMMUNICATION METHOD FOR SENDING A MESSAGE THROUGH A FIREWALL		
(57) Abstract <p>The invention is concerned with a method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall. The method comprises the following steps: a request with data for a new connection between the first computer system and at least one other computer system is sent from the first computer system to the firewall for a message to be sent between said computer systems. Up on approval of the connection by the firewall, information about necessary modifications to be made in a message that is sent via the requested connection through the firewall is sent from the firewall to the first computer system. The message to be sent is modified in the first computer system in accordance with the information sent from the firewall. Optionally, and before or after the foregoing step, identification data of the connection for the message to be sent between said computer systems is sent from the first computer system to the firewall so that the connection for the message can be identified by the firewall and the message can pass the firewall. The message is sent from the first computer system to the at least one other computer system through the firewall. The message to be sent between said computer systems can be protected after it has been modified, whereby the data to be sent from the first computer system to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.</p>		



09/913213

14

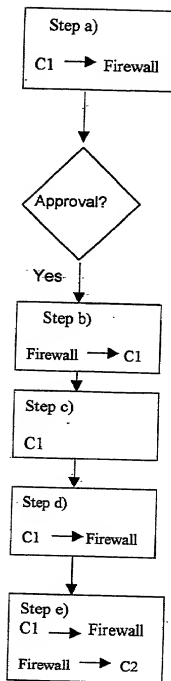


FIG. 1

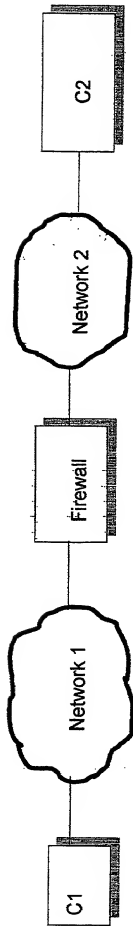


FIG. 2

AUG. 3.2001 8:19AM

FATH LAW OFFICES 3842882653

NO.939

P.9/12

RF 01 5/201 290 796USN



COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that.

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled DATA COMMUNICATION METHOD FOR SENDING A MESSAGE THROUGH A FIREWALL, the specification of which was filed as International Application No. PCT/FI00/00075 on February 3, 2000.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a). If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority
Claimed

990255
(Number)

Finland
(Country)

10 February 1999
(Day/Month/Year)

[X] []
Yes No

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations,

00913213-0129002

RFaj 8/201 250 726USN

§ 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(not applicable)	(n/a)	(not applicable)
(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

The undersigned hereby authorizes Rolf Fasth, the U.S. attorney named herein, to accept and follow instructions from Innopat Ltd. and/or Paivi Söderman as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between Rolf Fasth and the undersigned. In the event of a change in the persons from whom instructions may be taken, Rolf Fasth will be so notified by the undersigned.

① I hereby appoint Rolf Fasth, Registration No. 36,999, to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to Rolf Fasth at telephone number (904) 288-0262; fax number (904) 288-0263.

Address all correspondence to:

Rolf Fasth
FASTH LAW OFFICES
5255 Camelot Forest Drive
Jacksonville, FL 32258-2516

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

100

Full name of sole inventor: <u>Panu Pietikainen</u>
Inventor's signature <u>[Signature]</u> <u>August 28th, 2001</u> Date
Residence: <u>Espoo, Finland</u> <u>FTK</u>
Citizenship: <u>Finland</u>
Post Office address: <u>Taysikuu 10 C 103</u> <u>FIN-02210 Espoo, Finland</u>

09913213 012902